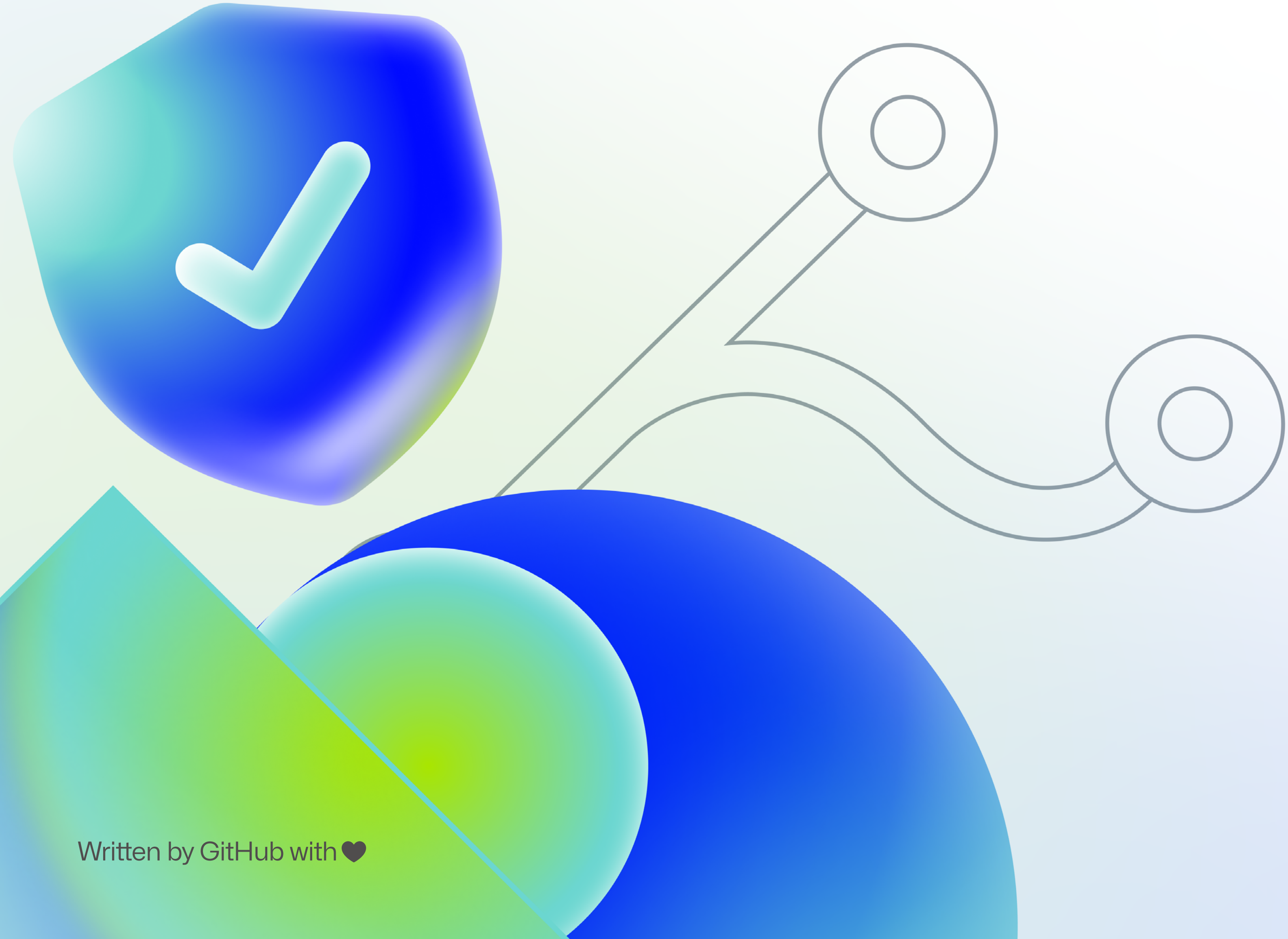
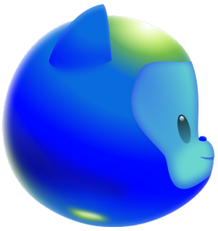
The enterprise guide to AI-powered DevSecOps



Written by GitHub with ♥

Table of contents



Foreword

DevSecOps is a practice and methodology that seeks to make shifting left a reality by integrating security into every step of the software development lifecycle (SDLC).

At its core, DevSecOps works to align security work, and in some cases, engineering and security roles that historically would be done separately, directly into the DevOps workflow.

As a result, DevSecOps reduces the cost and impact of security breaches, and enables teams to ship secure software faster. In fact, IBM's 2023 Cost of a Data Breach report cites a $1.68M cost savings for organizations with high DevSecOps adoption compared to those with low or no adoption.

The challenge of shifting left

Although security professionals have been encouraged to shift left for the past decade, the same IBM report found that only 33% of breaches were identified by an organization's internal security team. This shows how difficult it can be to incorporate security across the SDLC. In order to shift left, organizations need tools that not only can find security vulnerabilities before code goes into production, but can also seamlessly integrate into the SDLC.

How AI can help make shifting left a reality

When used effectively, AI can help prevent vulnerabilities from being written in the first place, provide secure code suggestions that developers can then test and refine, and provide context around potential vulnerabilities—all within the developer's typical workflow.

How this guide will help to create an AI-powered DevSecOps strategy

The IBM report concluded that DevSecOps was the top factor that helped companies reduce the average cost of a data breach. We've previously written about DevSecOps and best practices, and tips to help organizations integrate security practices throughout the SDLC. Now, let's discuss how AI can help to alleviate core challenges that organizations face when implementing a DevSecOps strategy: remediating risk efficiently, meeting increasing demand for security intelligence, and maintaining compliance with the latest regulatory standards.

3 core challenges with implementing DevSecOps and how AI can solve them

High DevSecOps adoption comes with high cost-saving benefits, but it's challenging to truly integrate security into the SDLC, rather than bolt on security tools to existing workflows.

The rapid adoption of AI in software development presents an opportunity to reduce friction in DevSecOps implementation. **By 2027, 50% of enterprise software engineers are expected to use machine-learning powered coding tools** according to Gartner. The adoption of these tools will cement AI's use throughout a DevSecOps workflow, paving the way for more efficient and proactive security practices.

Let's look at core challenges with implementing a DevSecOps strategy, discuss potential root causes, and then explore AI and automation solutions that can help organizations adopt a proactive security posture.

Challenge 1: Remediating security risks in the software supply chain

Financial investment alone doesn't remediate security risk. Remediation rates have remained stagnant over the years despite increased investment in security. Gartner predicts that **45% of global organizations will be impacted in some way by a supply chain attack by 2025.**

Applications and credential abuse are at the center of 86% of all data breaches, according to the 2023 Verizon Data Breach Investigation Report. And according to the IBM report, breaches from March 2022 to 2023 that began with stolen or compromised credentials took the longest to resolve—328 days to be exact. Even more, to meet deadlines, **81% of developers feel the pressure to release vulnerable code**, as cited in an Osterman Research white paper.

The key to protect against credential abuse? Adopt a DevSecOps strategy that ensures your platforms are secure by default through protections like multi-factor authentication and automated security controls. DevSecOps is the top factor that helps companies reduce the average cost of a data breach, according to the IBM report.

An estimated 45% **of global organizations will be impacted** by a supply chain attack by 2025.

86% **of all data breaches** occurred through applications and credential abuse in 2023.

A DevSecOps strategy is the top factor that helps companies reduce the average cost of a data breach.

How AI and automation can expedite remediation

The idea is not to replace security measures with AI. Rather, organizations can use AI to reduce friction and help augment their security programs. Let's look at a few AI and automation features that forward-thinking engineering leaders consider when selecting a DevSecOps platform:

- **Automating remediation alerts and suggesting code fixes.** A feature like a code scanning autofix can suggest an AI-generated code fix with vulnerability alerts in a pull request.
- **Protecting unstructured secrets.** Rather than scan identified and protected secrets only against predefined partner patterns, a capability like secret scanning can also detect passwords and other generic or unstructured secrets in code.
- **Auto-generating custom patterns.** Secret scanning can also use AI to auto-generate custom patterns and detect token types unique to an organization.

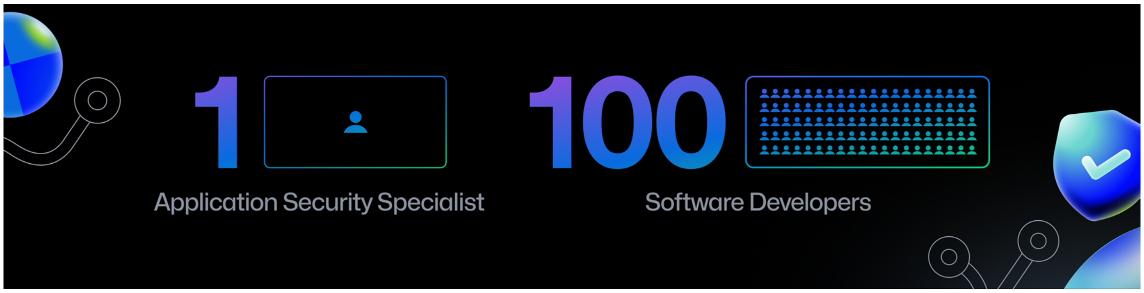
Did you know?

Automated security features can scan code, but an organization's security posture can change depending on where that feature comes in their SDLC. For instance, code can be scanned after it's published and trigger a security alert if a leaked secret is detected. On the other hand, a push protection feature can scan for secrets before code is pushed to an organization's repository.

A platform that supports proactive security features like push protection can prevent thousands of secret leaks. For example, GitHub Advanced Security's push protection feature prevented more than 11,000 secret leaks across 100 secret types from April to December 2022, according to internal data.

Challenge 2: Meeting the urgent demand for security intelligence

The world **needs 4 million more security professionals,** according to the 2023 workforce study from ISC2 (International Information System Security Certification Consortium). Exacerbating the demand is the ratio of developers to security professionals: **for every 100 developers, an organization has one security researcher**. If so much code is produced by a vast number of developers without enough security professionals to check it, vulnerabilities can be overlooked, leading to potential security breaches.



Additionally, with more enterprise software engineers expected to use AI coding tools, there will likely be more code to review, increasing demand for security professionals even more. But organizations can position themselves to keep up with the new landscape by implementing AI security practices into their security strategy.

How AI and automation can augment security intelligence

- **AI can help developers write safe code from the start.** AI coding tools can help developers make good security decisions in the flow of writing code, blending security and engineering together.

- **AI can augment manual efforts to hunt for threats.** For instance, advisory databases often include common vulnerability exposures and open source security advisories that are curated by security researchers. Robust security platforms may also have a vibrant community of bounty hunters in addition to a security incident response team that actively monitors data logging and telemetry sources for attacks. AI can accelerate those efforts allowing security researchers to perform research faster, helping them detect new vulnerabilities and automating manual processes.

- **AI can provide developers with security training and guidance.** When developers get a security alert, they can use products like AI coding tools directly in their workspace to understand what's wrong. That means instead of leaving their workspace to search the web for an answer, developers learn about security issues in the flow of their coding. Developers can also build familiarity with security concepts by using AI tools to generate vulnerability examples tailored to their codebase. This practical, hands-on learning experience allows developers to understand how a security issue manifests in code.

3 steps to turn collective security intelligence into results at scale

On average, 90% of organizations around the world use open source software (OSS), according to the Linux Foundation's Global Spotlight 2023 report. Additionally, the foundation found that 72% of companies planning to implement an OSPO or OSS initiative expect to do so within the next 12 months.

Securing OSS is a collective problem and a collective responsibility. That means a large, diverse group of developers, organizations, and individuals who depend on software, open source maintainers, and security experts all become stakeholders. Why does this matter? **Open source creates a larger pool of security intelligence to pull from.**

Here are three tips for turning collective security intelligence into results at scale:

1. **Provide engineering teams with hands-on security learning and development.** As mentioned above, an AI pair programmer can help developers learn more security concepts by generating vulnerability examples tailored to specific code. A free interactive training session, like Secure Code Game, also teaches developers how to spot and fix vulnerable patterns in real-world code, build security into workflows, and understand security alerts generated against code.

2. **Use a public database of advisories to secure private repositories.** Engineering leaders should select a platform that leverages security intelligence from a public advisory database. Such platforms can generate alert notifications when an advisory report is published about a vulnerability or malware that affects an organization's code.

3. **Accelerate understanding and modeling of OSS packages with AI.** There are thousands of packages in OSS, and they often contain APIs that may be unfamiliar to developers. But understanding and modeling those packages is what keeps the OSS ecosystem safe. Rather than modeling APIs manually, security and engineering teams can use AI tools to identify more packages and detect more vulnerabilities. Learn how a team of security researchers at GitHub discovered a new vulnerability using AI modeling.

Challenge 3: Meeting increasing compliance and regulatory standards

Organizations are facing increasing compliance and regulatory requirements that ensure the security and confidentiality of data and users. These standards are designed to minimize the risk of severe data breaches and cyber attacks, so demonstrating compliance assures customers that companies are committed to protecting personal data.

Here's an overview of several of those regulatory standards:

Executive Order on Safe, Secure and Trustworthy AI

Released in October 2023 by the Biden administration, the order provides a roadmap for the U.S. to design, develop, and deploy AI.

It emphasizes the development and use of trustworthy AI systems. It also encourages partnerships between the federal government, private sector, academia, and other stakeholders in developing and deploying AI.

Executive Order on Improving the Nation's Cybersecurity

Signed in May 2021 by the Biden administration, this executive order calls for tightening cybersecurity practices, as well as developing standards, guidelines, and procedures that set higher levels of software supply chain security.

HIPAA (Health Insurance Portability and Accountability Act

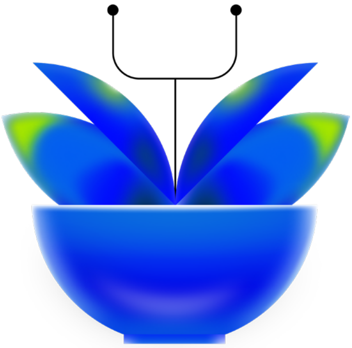
This U.S. law requires any U.S. business that handles protected health data to have secure electronic access to health data and to remain compliant with privacy regulations set by the U.S. Department of Health and Human Services.

Executive Order on Safe, Secure and Trustworthy AI

This European Union (EU) regulation places strict rules on how businesses collect and handle personal data, and it mandates that businesses protect the personal data and privacy of EU citizens and residents for transactions occurring within EU member states (even if the company itself isn't based in the EU).

PCI DSS (Payment Card Industry Data Security Standard)

Administered by the PCI Security Standards Council, this is a global set of information security standards for organizations that handle branded credit cards from the major card schemes.



GitHub: An AI-powered developer platform to build, scale, and deliver secure software

More than 100 million developers and more than 90% of the Fortune 100 companies use GitHub to build, maintain, and contribute to software projects. From empowering developers with the latest AI innovations to embedding security directly into the developer workflow, GitHub provides engineering teams with everything they need to build and deliver secure software.

Learn why teams choose GitHub >

How AI and automation can streamline compliance

Adhering to these standards creates a competitive advantage, so organizations need effective solutions that can assess and maintain compliance, and provide detailed reporting for audits. Here are the **top compliance tasks security tools should facilitate, and how AI and automation can help to streamline the process:**

Observability. A dashboard that provides macro-level visibility into an environment is critical to gauging the overall health and trends of an organization's security posture. By making it easy to locate alerts in the SDLC, a dashboard assists with risk tracking, remediation, and prevention. Dashboards can also highlight what teams are most effective with remediation and what kinds of vulnerabilities are being prevented with automation and AI features like secret scanning push protection. Additionally, enabling coding scanning by default in your organization's repositories allows for automated monitoring of codebases.

Reporting. The best solutions help teams automate compliance with industry standards, as well as provide detailed reports on vulnerabilities and compliance issues that can be shared with auditors. Platforms that provide easy access to detailed audit logs, compliance reports, and integrations support organizations in their internal and external compliance efforts.

Compliance management. Certifications from the International Organization for Standardization (ISO) like ISO 27701 and ISO 27018, and from the Cloud Security Alliance like STAR (Security, Trust & Assurance Registry), support data protection requirements in software development, ensure that developers follow best practices for data protection in cloud services, and assess the security of cloud services. Achieving and maintaining these certifications verifies commitment to maintaining high standards of data protection and security.

Selecting a platform with native AI and automated security features can help organizations meet those high standards while creating a positive DevSecOps experience. These tools can expedite remediations by prioritizing security alerts with custom and automated triage rules, allow organizations to catch insecure dependencies before they're introduced into an environment, and keep organizations informed about dependency licenses, changes, project use, and vulnerabilities.

Improve your security posture with GitHub Advanced Security

By leveraging GitHub Advanced Security features like dependency reviews, and code and secret scanning, organizations can better manage third-party libraries and dependencies, optimize workflows by integrating security directly into the SDLC, and maintain compliance with various industry regulations.

Secure your code today >

Implement your DevSecOps strategy with AI

Why do organizations need to secure the developer's workflow and adopt DevSecOps? Because software starts with code. Organizations that shift left and deeply integrate security into every step of the SDLC save $1.68M in costs compared to those with low or no DevSecOps adoption.

But as discussed above, there are challenges to implementing a successful DevSecOps strategy, including low remediation rates, an increasing demand for security professionals, and the need to meet increasing compliance and regulatory standards.

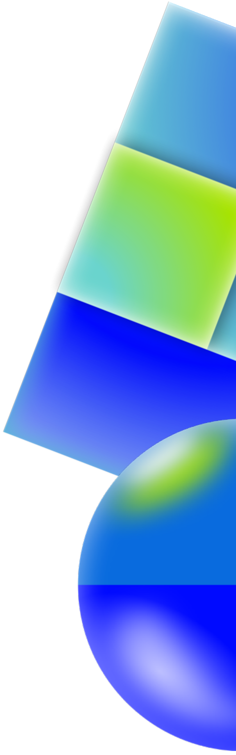
This is where AI and automation can help to make DevSecOps a reality:

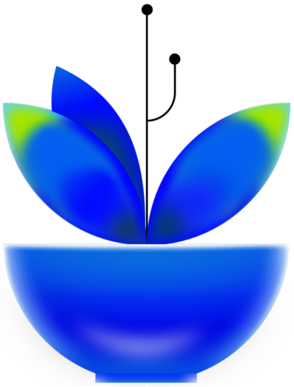
- **Expedite remediation.** AI coding tools can help developers write safer code from the start, while security tools can automate remediation alerts. When combined, alerts can include AI-generated code fix suggestions streamlining your developer's remediation workflow and boosting their productivity.
- **Augment collective security intelligence** by enabling security researchers to use AI to perform research faster and detect new vulnerabilities.
- **Improve developer security training** with an AI pair programmer that enables developers to learn about security issues in the flow of their coding, and with hands-on examples tailored to their codebase.
- **Improve monitoring, reporting, compliance management.** AI and automation tools can make it easy to pull audit logs and prioritize security alerts so that organizations can meet and maintain high compliance standards, all while improving the DevSecOps experience.

AI and automation security tools can play a crucial role in helping organizations secure code at the developer's desk. The result is reduced risk, faster detection and remediation, and faster deployments of more secure software.

GitHub is here to help. With GitHub Advanced Security, organizations can improve their security posture, optimize workflows, and proactively comply with various regulations and standards. Its AI-powered security features can also provide engineering teams with a frictionless DevSecOps experience, meaning businesses deliver products more securely and quickly.

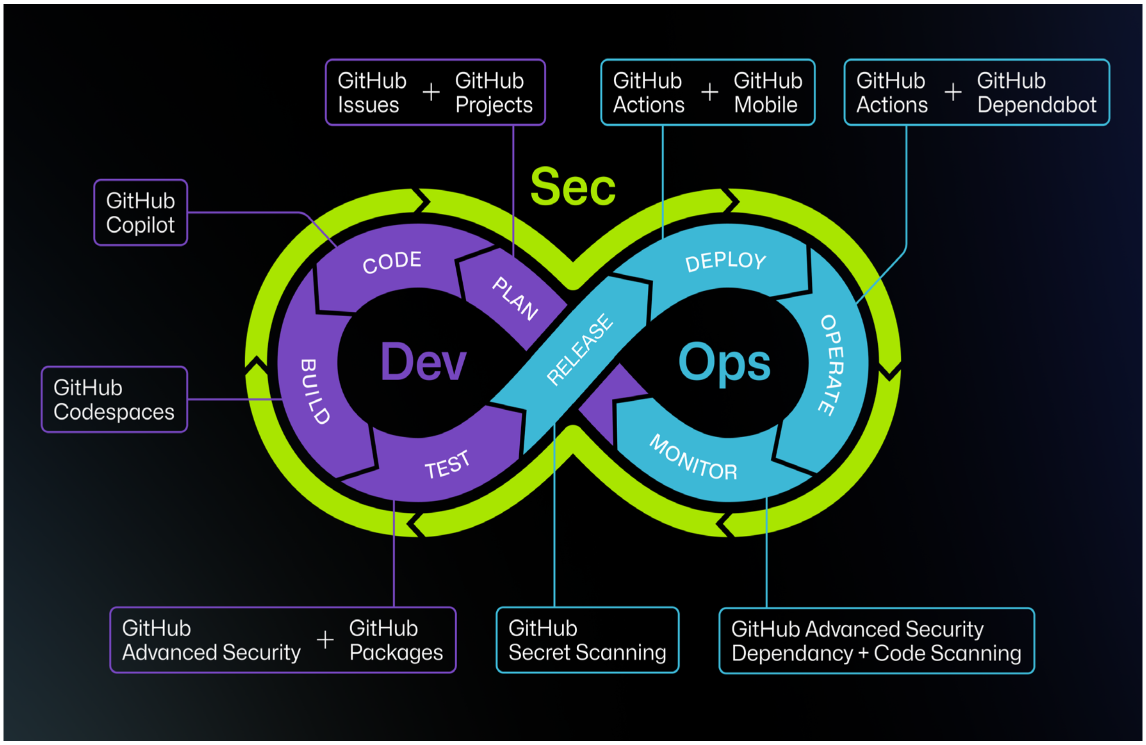
Learn more about GitHub Advanced Security >





Integrating AI-powered security at every step of the SDLC: A diagram

Security integration throughout the SDLC can help reduce friction when implementing a DevSecOps strategy. The diagram below shows how the GitHub platform provides a suite of security, AI, and automation tools and resources to improve the DevSecOps experience.


GitHub Issues + GitHub Projects
GitHub Actions + GitHub Mobile
GitHub Actions + GitHub Dependabot
Sec
GitHub Copilot
GitHub Codespaces
CODE
PLAN
Dev
BUILD
TEST
RELEASE
DEPLOY
Ops
OPERATE
MONITOR
GitHub Advanced Security + GitHub Packages
GitHub Secret Scanning
GitHub Advanced Security Dependancy + Code Scanning

Plan

Together, GitHub Issues and GitHub Projects offer an integrated toolset to plan, organize, track, and manage your projects right within GitHub, streamlining any project management process. For instance, project managers can create GitHub Project boards to automate tracking of security-related issues and pull requests.

Code

By recommending secure practices, catching errors early on, and minimizing common coding errors, GitHub Copilot can help developers write more secure code from the start. It's important to note that AI is there to assist with code writing and should not replace thorough security reviews and good coding practices.

Build

GitHub Codespaces provides developers across teams with consistent, pre-configured build environments that are designed to be secured by default.

Test

GitHub Advanced Security and GitHub Packages can work together to streamline the testing process. For instance, GitHub Advanced Security features help developers to address security concerns before code changes are merged, detect secrets before they're pushed to repositories, and spot and address potential security risks in their dependencies. Meanwhile, GitHub Packages enable developers to host software packages, making it more straightforward to replicate real-world environments for testing and therefore enhancing the effectiveness of testing.

Release

GitHub Advanced Security features like secret scanning ensure no sensitive information is included in code before it's deployed. Developers can use secret scanning's AI features to help generate custom patterns to protect secret types that are unique to an organization.

Deploy

GitHub Actions and GitHub Mobile provide enhanced safeguards and faster response capability, which create a more secure deployment process. For instance, organizations can use GitHub Actions to automatically execute linters, static analysis tools, or security vulnerability scans whenever code is pushed or a pull request is made. GitHub Mobile, while it doesn't provide deployment features, can be used for monitoring the deployment process and reacting quickly if manual intervention is required during deployment.

Operate and monitor

Using tools like GitHub Actions, Dependabot, and GitHub Advanced Security enable organizations to identify, remediate, and prevent security vulnerabilities in an efficient and timely manner. For instance, GitHub Actions can automate the running of security checks and scans, as well as deployment processes to ensure that only tested and secure code is deployed. GitHub Advanced Security's dependency review and Dependabot monitor dependencies for changes, project integration, and vulnerabilities. GitHub Advanced Security's code scanning autofix feature can provide AI-generated code fixes alongside vulnerability alerts in a pull request.

Let's build from here

The world's leading AI-powered developer platform.

100+ million
Developers

4+ million
Organizations

420+ million
Repositories

90%
Fortune 100

Follow us on